II. AMENDMENTS TO THE SPECIFICATION

Please amend paragraph 012 as follows:

[012] DoS defense system 12 may be implemented as a standalone system, as a software program product, or be integrated into web server 10. In such implementations, DoS defense system 12 can be configured to act as a "front-end" to most of the server processes [[~~14~~]] 24 that handle requests 20 sent to the web server 10. Thus, if an attack occurs, most server processes [[~~14~~]] 24 of web server 10 will not affected or utilized. It should be understood that while the present invention is described with reference to a web server 10 that receives and responds to requests, the invention could be implemented with any web resource that receives and responds to any type of message using a hypertext transfer protocol (HTTP), or similar communications protocol.

Please amend paragraph 013 as follows:

[013] DoS defense system 12 includes an improper request detection system 14, a tracking database 18, and a DoS response system 16 that includes a DoS response protocol 17. Improper request detection system 14 can include any logic that examines incoming requests 20 and determines if the request 20 appears to be improper. In the case of a typical application server known in the art, identifying improper requests is a relatively simple operation since the source and format of requests 20 are generally limited and known. For instance, a request may be deemed improper if: (1) it is received from an unexpected host, such as www; (2) if the received packet has a zero length; (3) if the received packet is neither an HTTP "post" or "get" command

when only these commands are expected; or (4) if the request comprises "post" or "get" arguments unknown to the web server 10. In the event the request is deemed proper or good, it is passed to the standard set of server processes [[~~14~~]] 24 for processing. Alternatively, if the request appears to be improper of bad, the request is passed to DoS response system 16. Furthermore, source information from all improper requests are stored in memory and/or a tracking database 18 so that improper requests from the same source can be identified and dealt with as an apparent DoS attack.